REPUBLIC OF FRANCE

Publication No.: 2 732 537
(indicate only when ordering reprints)

National Institute for Industrial Property
PARIS

National File No.: 95 03859

Int. Cl.[6] : H 04 N 7/16. 9/76,
G 09 C 1/00

# PATENT APPLICATION A1

**Filing date :** 31 March 1995

**Priority :**

**Date at which the application was laid open to the public :** 4 October 1996 Bulletin 96/40

**List of documents cited in the preliminary search report:** see report at end of section

**References to other national published documents :**

**Applicant :** *CANAL + SOCIETE ANONYME -*

**Inventor(s) :** DUVERNE JACQUES

**Proprietor(s) :**

**Representative(s) :** SABATIER

(54) Process and Installation of Encrypted Digital Data Recording

(57) A process for recording encrypted digital data, especially for television programs, permitting protecting the interests of those having rights to broadcast works.

According to the invention the digital data is recorded in a register (17) in scrambled form after having replaced the scrambling key of the operating components of said digital data by an equivalent encoded scrambling key by an internal operating key (Cexi) specific to the decryption unit associated with the recorder, the substitution of the keys being possible to carry out by means of a shift register (18).

"Process and installation of encrypted digital data recording."

The invention relates to a process for recording encrypted digital data, especially for television programs broadcast in encrypted form from a broadcasting center to decryption units where the digital data may be decoded and restored in clear, for example on a television screen.

The invention also concerns a digital data recording system associating means of decryption with a digital recorder.

It is known that the recording of television programs may be done virtually without loss of quality. A result of this is a legitimate concern of those holding the rights of audiovisual works which may be broadcast in digital form, by radio waves or by cable. In fact, a single broadcast of a work over such a network may give rise to an activity of the production of perfectly reproducible copies indefinitely and without degradation to supply illegally a pirate recording market. Up to the present, highly imperfect solutions have been put into operation. One of them comprises characterizing each copy put legally into circulation by a "signature" which permits going back to the incorrect one in the case of massive unauthorized broadcast. This practice permits repressing criminal acts but does not prevent commercial piracy.

Moreover, the recording of such works in view of a private usage limited according to the dedicated expression, to the "family circle" i.e. devoid of commercial nature, has long been tolerated and must be able to be pursued with the advent of digital television.

The invention permits by the expedient of encrypted broadcasting making an equitable compromise between the legitimate interests of those holding the rights of broadcast works and the respect of freedom to copy for private use.

More precisely, the invention concerns a process for recording encrypted digital data, for example television data, broadcast in encrypted form from a broadcasting center including means of encryption parameterized by a scrambling key to at least one decryption unit including means of unscrambling, said digital data including operating components (ECM) defining a scrambling key encoded by an operating key, characterized in that it is comprised of recording said digital data in scrambled form after having replaced the encoded scrambling key in said operating components by an equivalent scrambling key encoded by an internal operating key specific to said decryption unit.

According to a preferred mode of implementation, the process comprises decoding the scrambling key valid at a given moment in each operating component, in encoding it again under the parameterization of said internal operating key and in reinserting it under this new encoded form in each operating component instead of said valid scrambling key.

The invention likewise concerns an installation of encrypted digital data recording, for example television programs broadcast in encrypted form from a broadcasting center including encryption means parameterized by a scrambling key of the type including a digital recorder connected to a decryption unit comprising means of unscrambling, said digital data including operating components (ECM) defining a scrambling key encoded by an operating key, characterized in that the recording input of said digital recorder is connected to a transmission line of said scrambled digital data via means of substitution able to replace said scrambling key from an operating component by an equivalent scrambling key parameterized by an internal operating key specific to said decryption unit.

The invention will be better understood and other advantages of the latter will appear more clearly in light of the description which will be followed by one possible embodiment example according to its principle, given solely by way of example and

carried out in reference to the attached drawings in which:

- Figure 1 is a schematic block diagram illustrating an encrypted digital data broadcasting system with a decryption unit which can receive, decode, and use these data,

- Figure 2 illustrates the nature of the transmitted digital data; and,

- Figure 3 illustrates in the form of a block diagram the means specific to the invention which make up each decryption unit to permit the recording according to the principle of the invention.

A digital data encrypted transmission system, in particular for digital picture television programs, is illustrated. It includes an encryption unit 11 associated with a broadcasting center and a decryption unit 12 entrusted to a subscriber and representing a decoder; this decryption unit is connected to a receiver 13 for display, typically of a television receiver, after digital - analog conversion. Each subscriber therefore has such a decryption unit 12. A communications network 15 is established between the encryption unit 11 and the decryption unit or decoder 12. This involves for example a radio wave broadcasting system which may be relayed by satellite, or a program distribution cable network.

The digital data N representative of a program are comprised, as shown in Figure 2, of a succession of messages transmitted sequentially and each including a component V representative of the picture, a component S representative of the sound, [and] where applicable a component T including Teletext data. The broadcasting is called "access controlled" when at least one component V, S, or T (generally all three) is scrambled upon broadcasting. Operating components henceforth called "ECM components" (from the English "entitlement control message") complete the components identified above to form each time a predetermined message. It should be noted that very generally the

communications network 15 transmits simultaneously a multiplicity of programs, encrypted or not. The messages of data representative of these programs are multiplexed upon broadcast by a multiplexer Mp and each decoder comprises an input demultiplexer DMp tasked with restoring the data (according to the configuration of Figure 2) corresponding to the program selected by the subscriber. The multiplexer Mp receives therefore among other things the data delivered by a scrambler E from the encryption unit 11. This scrambler receives at an input e the digital data N and subjects it to an algorithm using a parameter called the "scrambling key" Ce.

This scrambling key is delivered to the scrambler and in encoded form by an encoder $Ch_1$ is sent to the decryption unit 12 via the communications network 15 to control a decoder $Dch_1$ able to restore the key Ce which is applied as the parameter to an unscrambler D of the decryption unit 12. This unscrambler in the presence of the same key Ce which is validated upon emission is able to subject the digital data received from the demultiplexer DMp to an algorithm inverse to that of the scrambler to restore the digital data in clear. The latter are applied to an input of the receiver 13 (via means of digital - analog conversion, not represented) to be reproduced, here as a television program.

The cryptogram of the scrambling key Ce enters into the constitution (with the criteria of access to the scrambled component(s)) of the ECM components indicated above. For security the scrambling key is modified periodically (for example every 10 seconds) by the encoder $Ch_1$ under the command of an operating key Cex. The latter is also encoded by an encoder $Ch_2$ so as to be transmitted for example by downloading to the decryption unit 12 to a decoder $Dch_2$ able to restore the operating key Cex applicable to the decoder $Dch_1$.

As stated previously, the scrambling key Ce changes rather frequently (10 seconds) to fight effectively against piracy; it is repeated several times per second in the ECMs to permit an immediate decoding when the subscriber selects the corresponding program.

On the other hand, the operating key Cex is only changed at the end of a longer time period, for example of the order of a month. This operation is performed under the control of a management key Cg which is personalized for each subscriber.

The different keys Ce, Cex, and decoders $Dch_1$, $Dch_2$ associated with them are integrated into a security module of the decryption unit 12 and are thus inaccessible to the holder of the decoder.

The invention belongs within the scope of operation of a system of this type and has as its objective permitting copying a program in digitized form for the purpose of exclusively private use. In fact, it is known that the recording of a digital video program can be done practically without degradation of quality and that a broadcaster of such digitized programs may become a source for duplication, inflicting loss and damage to those holding rights to the broadcast audiovisual works.

In such a system there has never been considered up to now recording the program in its scrambled form. In fact, such a program would be no longer readable after the first change of the operating key arising after its recording.

The fundamental idea of the invention comprises, on the other hand, making use of a digital recording of a program in scrambled form and using this scrambling to reserve the re-reading to the exclusive use of a subscriber who has made said recording. To do this, the decryption unit 12 includes a shift 16 of the scrambled digital signal upstream from the unscrambler D connected to the recording line of a digital recorder 17 such as a videotape recorder and in which are switched means of substitution of the ECM components able to replace the ECMs which are transmitted by new ECMs comprising an equivalent scrambling key encoded by an operating key called "internal" Cexi intrinsic to the subscriber. This key Cexi which is specific is different for each one of the users, i.e. integrated into the security module of the decoder. In practice these means will be, for example, comprised of a simple shift register 18 (Figure 3) into which flow

the messages coming from the output of the multiplexer DMp. When the ECM component of a message passes through this shift register, the resetting inputs Fi are commanded to place all of the stages concerned of the register in states representing a scrambling key encoded by said internal operating key.

More precisely, the unscrambler D comprises an output where the scrambling key Ce, valid at a given moment of the recording, is available. This scrambling key controls an internal encoder Chi parameterized by the internal operating key Cexi. The output of the internal encoder controls the resetting inputs of the shift register to record the cryptogram of the new scrambling key encoded by the internal operating key Cexi. The other scrambled components V, S, and T are not modified and the succession of messages representing a program is recorded in this form, i.e. with the ECM components modified as indicated.

Upon reproduction it suffices to connect the digital output of the recorder to the input of the unscrambler D and to parameter the decoder $Dch_1$ by the internal operating key Cexi replacing the key Cex.

## Patent Claims

1. A process for recording encrypted digital data, for example television data broadcast in encrypted form from a broadcasting center (11) including means of encryption parameterized by a scrambling key to at least one decryption unit (12) including means of unscrambling, said digital data including operating components (ECM) defining a scrambling key (Ce) encoded by an operating key, characterized in that it is comprised of recording (17) said digital data in scrambled form after having replaced the encoded scrambling key in said operating components by an equivalent scrambling key encoded by an internal operating key (Cexi) specific to said decryption unit.

2. A process according to claim 1, characterized in that it is comprised of decoding said scrambling key (Ce) valid in each operating component, in encoding it (Chi) again under the parameterization of said internal operating key, and in reinserting it (18) in this new encoded form in each operating component instead of said valid scrambling key.

3. A process according to claim 2, characterized in that it consists of having said scrambled digital data circulate in a shift register (18), before recording it and in controlling the resetting inputs (Fi) of said shift register to record in them said equivalent scrambling key when said register includes said valid scrambling key.

4. The installation of encrypted digital data recording, for example television programs, broadcast in encrypted form from a broadcasting center (11) including means of encryption parameterized by a scrambling key, of the type including a digital recorder (17) connected to a decryption unit comprising means of unscrambling (D), said digital data including operating components (ECM) defining a scrambling key encoded by an operating key, characterized in that the recording input of said digital recorder (17) is connected to a transmission line of said scrambled digital data via substitution means (18) able to replace said scrambling key of an operating component by an equivalent scrambling key parameterized by an internal operating key (Cexi) specific to said decryption unit (12).

5. An installation according to claim 4, characterized in that said transmission line (16) of said scrambled digital data is connected upstream from said means of scrambling and comprises a shift register (18) in which pass said scrambled digital data, [and] in that said means of unscrambling comprise an output where there is delivered said scrambling key (Ce) decoded and in that an internal encoder (Chi) controls means of resetting said shift register, said internal encoder being connected to said output delivering said decoded scrambling key.

6. An installation according to claim 5, characterized in that the internal encoder (Chi) is parameterized by said internal operating key (Cexi) and delivers resetting data to the shift register representing said scrambling key encoded by said internal operating key when said register comprises scrambling key data for an operating component (ECM).

THIS PAGE BLANK (USPTO)

FRENCH REPUBLIC

# Preliminary Search Report

2732537
National Application No.

NATIONAL INSTITUTE
OF INTELLECTUAL PROPERTY

FA 516352
FR 9503859

## Relevant Documents

| Category | Identification of Documents with specification, where required of critical parts | Re Claim |
|---|---|---|
| A | CABLE TV SESSIONS, MONTREUX, JUNE 10 - 15, 1993,<br>No. SYMP. 18, 11 June 1993<br>POSTES; TELEPHONES ET TELEGRAPHES SUISSES,<br>page 761-769, XP 000379391<br>VIGARIE J P 'A DEVICE FOR REAL-TIME MODIFICATION OF ACCESS CONDITIONS IN A D2-MAC/PACKET EUROCRYPT SIGNAL: THE TRANSCONTROLLER'<br>* the entire document * | 1-6 |
| A | PATENT ABSTRACTS OF JAPAN<br>Vol. 014 No. 200 (E-0920), 24 April 1990 &<br>JP-A-02 041051 (MATSUSHITA ELECTRIC IND CO LTD; OTHERS: 01) 9 February 1990,<br>* Abstract * | 1-6 |
| A | US-A-5 230 019 (YANAGIMICHI TOYOKAZU ET AL)<br>20 July 1993<br>* Abstract * | 1-6 |
| A | EP-A-0 461 029 (MATRA COMMUNICATION; FRANCE TELECOM (FR); TELEDIFFUSION FSE (FR)) 11 December 1991<br>* the entire document * | 1-6 |

Searched Fields (Int. Cl. 6)

H04N

The present search report was completed for all patent claims

| Search completed | Examiner |
|---|---|
| 9 October 1995 | Greve, M |

Category of cited documents

A pertinent in opposition to more than one claim or general background technology

THIS PAGE BLANK (USPTO)

RCA 89181

CITED BY APPLICANT

(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 732 537**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **95 03859**

(51) Int Cl⁶ : H 04 N 7/16, 9/76, G 09 C 1/00

# (12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 31.03.95.

(30) **Priorité** :

(43) **Date de la mise à disposition du public de la demande** : 04.10.96 Bulletin 96/40.

(56) **Liste des documents cités dans le rapport de recherche préliminaire** : *Se reporter à la fin du présent fascicule.*

(60) **Références à d'autres documents nationaux apparentés** :

(71) **Demandeur(s)** : *CANAL + SOCIETE ANONYME* — FR.

(72) **Inventeur(s)** : DUVERNE JACQUES.

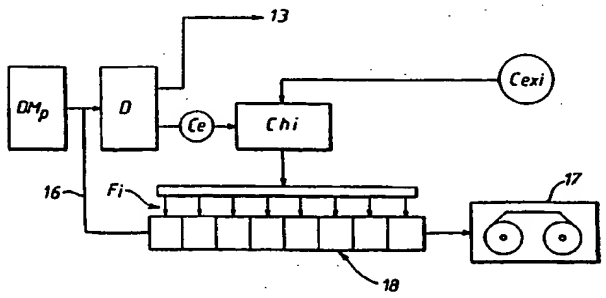
(73) **Titulaire(s)** :

(74) **Mandataire** : SABATIER.

## (54) PROCEDE ET INSTALLATION D'ENREGISTREMENT D'INFORMATIONS NUMERIQUES CRYPTEES.

(57) Procédé d'enregistrement d'informations numériques cryptées, notamment des programmes de télévision, permettant de préserver les intérêts des ayants droit des oeuvres diffusées.

Selon l'invention, on enregistre dans un enregistreur (17) les informations numériques sous forme embrouillée après avoir remplacé la clé d'embrouillage des composantes d'exploitation desdites informations numériques par une clé d'embrouillage équivalente chiffrée par une clé d'exploitation interne (Cexi) spécifique à l'unité de décryptage associée à l'enregistreur, la substitution des clés pouvant se faire au moyen d'un registre à décalage (18).




FR 2 732 537 - A1

"Procédé et installation d'enregistrement d'informations numériques cryptées"

L'invention se rapporte à un procédé d'enregistrement d'informations numériques cryptées, notamment des programmes de télévision, diffusées sous forme cryptée depuis un centre d'émission jusqu'à des unités de décryptage où les informations numériques peuvent être décodées et restituées en clair, par exemple sur un écran de télévision.

L'invention concerne aussi une installation d'enregistrement d'informations numériques associant des moyens de décryptage à un enregistreur numérique.

On sait que l'enregistrement de programmes de télévision peut se faire pratiquement sans perte de qualité. Il en résulte une inquiétude légitime des ayants droit des oeuvres audiovisuelles susceptibles d'être diffusées sous forme numérique, par voie hertzienne ou par câble. En effet, une seule diffusion d'une oeuvre sur un tel réseau peut donner naissance à une activité de production de copies parfaitement reproductibles indéfiniment et sans dégradation, pour alimenter illégalement un marché d'enregistrements pirates. Jusqu'à présent, des solutions très imparfaites ont été mises en oeuvre. L'une d'elles consiste à caractériser chaque copie mise légalement en circulation par une "signature" qui permet de remonter jusqu'au fautif en cas de diffusion massive non autorisée. Cette pratique permet de réprimer

des agissements délictueux mais ne permet pas de prévenir le piratage commercial.

Par ailleurs, l'enregistrement de telles oeuvres en vue d'un usage privé, limité, selon l'expression consacrée, au "cercle familial", c'est-à-dire dépourvu de caractère commercial, est depuis longtemps toléré et doit pouvoir se poursuivre avec l'avènement de la télévision numérique.

L'invention permet, par le biais de la diffusion cryptée, de proposer un compromis équitable entre les intérêts légitimes des ayants droit des oeuvres diffusées et le respect de la liberté de copie à usage privé.

Plus précisément, l'invention concerne un procédé d'enregistrement d'informations numériques cryptées, par exemple des informations de télévision, diffusées sous forme cyptée depuis un centre d'émission comprenant des moyens de cryptage paramétrés par une clé d'embrouillage jusqu'à au moins une unité de décryptage comprenant des moyens de désembrouillage, lesdites informations numériques renfermant des composantes d'exploitation (ECM) définissant une clé d'embrouillage chiffrée par une clé d'exploitation, caractérisé en ce qu'il consiste à enregistrer lesdites informations numériques sous forme embrouillée après avoir remplacé la clé d'embrouillage chiffrée dans lesdites composantes d'exploitation par une clé d'embrouillage équivalente chiffrée par une clé d'exploitation interne, spécifique à ladite unité de décryptage.

Selon un mode d'exploitation préféré, le procédé consiste à déchiffrer la clé d'embrouillage valide à un

moment donné dans chaque composante d'exploitation, à la chiffrer à nouveau sous le paramétrage de ladite clé d'exploitation interne et à la réinsérer sous cette nouvelle forme chiffrée dans chaque composante d'exploitation à la place de ladite clé d'embrouillage valide.

L'invention concerne également une installation d'enregistrement d'informations numériques cryptées, par exemple des programmes de télévision, diffusées sous forme cryptée depuis un centre d'émission comprenant des moyens de cryptage paramétrés par une clé d'embrouillage, du type comprenant un enregistreur numérique relié à une unité de décryptage comportant des moyens de débrouillage, lesdites informations numériques renfermant des composantes d'exploitation (ECM) définissant une clé d'embrouillage chiffrée par une clé d'exploitation, caractérisée en ce que l'entrée d'enregistrement dudit enregistreur numérique est connectée à une ligne de transmission desdites informations numériques embrouillées via des moyens de substitution aptes à remplacer ladite clé d'embrouillage d'une composante d'exploitation par une clé d'embrouillage équivalente paramétrée par une clé d'exploitation interne, spécifique à ladite unité de décryptage.

L'invention sera mieux comprise et d'autres avantages de celle-ci apparaîtront plus clairement à la lumière de la description qui va suivre d'un exemple de réalisation possible conforme à son principe, donnée uniquement à titre d'exemple, et faite en référence aux dessins annexés dans

lesquels:

- la figure 1 est un schéma-bloc de principe illustrant un système de diffusion d'informations numériques cryptées avec une unité de décryptage susceptible de recevoir, décoder et exploiter ces informations;

- la figure 2 illustre la nature des informations numériques transmises; et

- la figure 3 illustre, sous forme de schéma-bloc, les moyens spécifiques à l'invention, qui complètent chaque unité de décryptage pour permettre l'enregistrement conforme au principe de l'invention.

Un système de transmission cryptée d'informations numériques, en particulier de programmes de télévision à images numérisées est illustré. Il comprend une unité de cryptage 11 associée à un centre d'émission et une unité de décryptage 12 confiée à un abonné et constituant un décodeur; cette unité de décryptage est reliée à un récepteur 13 de visualisation, typiquement un récepteur de télévision, après conversion numérique-analogique. Chaque abonné possède donc une telle unité de décryptage 12. Un réseau de communication 15 est établi entre l'unité de cryptage 11 et l'unité de décryptage ou décodeur 12. Il s'agit par exemple d'un système de transmission par faisceau Hertzien, éventuellement relayé par satellite, ou d'un réseau câblé de distribution de programmes.

Les informations numériques N représentatives d'un programme sont constituées, comme le montre la figure 2,

d'une succession de messages transmis séquentiellement et comportant chacun une composante V représentative de l'image, une composante S représentative du son, éventuellement une composante T renfermant des informations de télétexte. La diffusion est dite "à accès contrôlé" lorsqu'au moins une composante V, S ou T (généralement les trois) est embrouillée à l'émission. Des composantes d'exploitation appelés ci-après "composantes ECM", (de l'anglais "Entitlement Control Message") complètent les composantes identifiées ci-dessus pour former, chaque fois, un message précité. Il est à noter que, très généralement, le réseau de communication 15 transmet simultanément une pluralité de programmes, cryptés ou non. Les messages d'informations représentatifs de ces programmes sont multiplexés à l'émission par un multiplexeur Mp et chaque décodeur comporte un démultiplexeur d'entrée DMp chargé de restituer les informations (selon la configuration de la figure 2) correspondant au programme choisi par l'abonné. Le multiplexeur Mp reçoit donc, entre autres, les informations délivrées par un embrouilleur E de l'unité de cryptage 11. Cet embrouilleur reçoit sur une entrée e les informations numériques N et les soumet à un algorithme mettant en oeuvre un paramètre dit "clé d'embrouillage" Ce.

Cette clé d'embrouillage est délivrée à l'embrouilleur et sous forme chiffrée par un chiffreur $Ch_1$ est adressée à l'unité de décryptage 12, via le réseau de communication 15 pour piloter un déchiffreur $Dch_1$ apte à restituer la clé Ce qui est appliquée en tant que paramètre à un

désembrouilleur D de l'unité de décryptage 12. Ce désembrouilleur, en présence de la même clé Ce, qui est validée à l'émission, est capable de soumettre les données numériques reçues du démultiplexeur DMp à un algorithme inverse de celui de l'embrouilleur pour restituer les informations numériques en clair. Celles-ci sont appliquées à une entrée du récepteur 13, (via des moyens de conversion numérique/analogique, non représentés) pour être reproduites, ici en tant que programme de télévision.

Le cryptogramme de la clé d'embrouillage Ce entre dans la constitution (avec les critères d'accès à la ou les composantes embrouillées) des composantes ECM indiqués ci-dessus. Par sécurité, la clé d'embrouillage est modifiée périodiquement (par exemple toutes les 10 secondes), par le chiffreur $Ch_1$ sous la commande d'une clé d'exploitation Cex. Celle-ci est aussi chiffrée par un chiffreur $Ch_2$ de façon à être transmise, par exemple par téléchargement, à l'unité de décryptage 12, jusqu'à un déchiffreur $Dch_2$ capable de restituer la clé d'exploitation Cex applicable au déchiffreur $Dch_1$.

Comme mentionné précédemment, la clé d'embrouillage Ce change assez fréquemment (10 secondes) pour lutter efficacement contre le piratage; elle est répétée plusieurs fois par seconde dans les ECM pour permettre un décodage immédiat dès que l'abonné sélectionne le programme correspondant. En revanche, la clé d'exploitation Cex n'est modifiée qu'au bout d'une période de temps plus longue, par exemple de l'ordre d'un mois. Cette opération se fait sous

le contrôle d'une clé de gestion Cg personnalisée pour chaque abonné.

Les différentes clés Ce, Cex et déchiffreurs $Dch_1$, $Dch_2$ associés sont intégrés dans un module de sécurité de l'unité de décryptage 12, et sont donc inaccessibles au détenteur du décodeur.

L'invention s'inscrit dans le cadre de l'exploitation d'un système de ce genre et vise à permettre la copie d'un programme sous forme numérisée en vue d'un usage exclusivement à titre privé. En effet, on sait que l'enregistrement vidéo d'un programme numérisé peut être fait pratiquement sans dégradation de qualité et qu'un diffuseur de tels programmes numérisés pourrait devenir une source de duplication, portant préjudice aux ayants droit des oeuvres audiovisuelles diffusées.

Dans un tel système, on n'a jusqu'à présent jamais envisagé d'enregistrer le programme sous sa forme embrouillée. En effet, un tel programme ne serait plus lisible après le premier changement de la clé d'exploitation intervenant après son enregistrement.

L'idée de base de l'invention consiste au contraire à tirer parti d'un enregistrement numérique d'un programme sous forme embrouillée en utilisant cet embrouillage pour réserver la relecture à l'usage exclusif de l'abonné qui a réalisé ledit enregistrement. Pour ce faire, l'unité de décryptage 12 comporte une dérivation 16 de signal numérique embrouillé, en amont du désembrouilleur D, reliée à la ligne d'enregistrement d'un enregistreur numérique 17

tel qu'un magnétoscope et dans laquelle sont intercalés des moyens de substitution des composantes ECM, aptes à remplacer les ECM qui sont transmis, par de nouveaux ECM contenant une clé d'embrouillage équivalente chiffrée par une clé d'exploitation dite "interne" Cexi, propre à l'abonné. Cette clé Cexi, spécifique, est différente pour chacun des usagers, c'est-à-dire intégrée au module de sécurité du décodeur. Dans la pratique, ces moyens seront par exemple constitués par un simple registre à décalage 18 (figure 3) dans lequel défilent les messages issus de la sortie du multiplexeur DMp. Lorsque la composante ECM d'un message traverse ce registre à décalage, les entrées de forçage Fi sont commandées pour placer tous les étages concernés du registre dans des états représentant une clé d'embrouillage chiffrée par ladite clé d'exploitation interne.

Plus précisément, le désembrouilleur D comporte une sortie où la clé d'embrouillage Ce, valide à un moment donné de l'enregistrement, est disponible. Cette clé d'embrouillage pilote un chiffreur interne Chi paramétré par la clé d'exploitation interne Cexi. La sortie du chiffreur interne pilote les entrées de forçage du registre à décalage pour inscrire le cryptogramme de la nouvelle clé d'embrouillage chiffrée par la clé d'exploitation interne Cexi. Les autres composantes embrouillées V, S et T ne sont pas modifiées et la succession des messages représentatifs d'un programme est enregistrée sous cette forme, c'est-à-dire avec des composantes ECM modifiées comme indiqué.

A la reproduction, il suffit de brancher la sortie numérique de l'enregistreur à l'entrée du désembrouilleur D et de paramétrer le déchiffreur $Dch_1$ par la clé d'exploitation interne Cexi, se substituant à la clé Cex.

REVENDICATIONS

1- Procédé d'enregistrement d'informations numériques cryptées, par exemple des informations de télévision diffusées sous forme cyptée depuis un centre d'émission (11) comprenant des moyens de cryptage paramétrés par une clé d'embrouillage jusqu'à au moins une unité de décryptage (12) comprenant des moyens de désembrouillage, lesdites informations numériques renfermant des composantes d'exploitation (ECM) définissant une clé d'embrouillage (Ce) chiffrée par une clé d'exploitation, caractérisé en ce qu'il consiste à enregistrer (17) lesdites informations numériques sous forme embrouillée après avoir remplacé la clé d'embrouillage chiffrée dans lesdites composantes d'exploitation par une clé d'embrouillage équivalente chiffrée par une clé d'exploitation interne (Cexi), spécifique à ladite unité de décryptage.

2- Procédé selon la revendication 1, caractérisé en ce qu'il consiste à déchiffrer ladite clé d'embrouillage (Ce) valide dans chaque composante d'exploitation, à la chiffrer (Chi) à nouveau sous le paramétrage de ladite clé d'exploitation interne et à la réinsérer (18) sous cette nouvelle forme chiffrée dans chaque composante d'exploitation à la place de ladite clé d'embrouillage valide.

3- Procédé selon la revendication 2, caractérisé en ce qu'il consiste à faire circuler lesdites informations numériques embrouillées dans un registre à décalage (18),

avant de les enregistrer et à piloter des entrées de forçage (Fi) dudit registre à décalage pour y inscrire ladite clé d'embrouillage équivalente lorsque ledit registre renferme ladite clé d'embrouillage valide.

4- Installation d'enregistrement d'informations numériques cryptées, par exemple des programmes de télévision, diffusées sous forme cryptée depuis un centre d'émission (11) comprenant des moyens de cryptage paramétrés par une clé d'embrouillage, du type comprenant un enregistreur numérique (17) relié à une unité de décryptage comportant des moyens de débrouillage (D), lesdites informations numériques renfermant des composantes d'exploitation (ECM) définissant une clé d'embrouillage chiffrée par une clé d'exploitation, caractérisée en ce que l'entrée d'enregistrement dudit enregistreur numérique (17) est connectée à une ligne de transmission desdites informations numériques embrouillées via des moyens de substitution (18) aptes à remplacer ladite clé d'embrouillage d'une composante d'exploitation par une clé d'embrouillage équivalente paramétrée par une clé d'exploitation interne (Cexi), spécifique à ladite unité de décryptage (12).

5- Installation selon la revendication 4, caractérisée en ce que ladite ligne de transmission (16) desdites informations numériques embrouillées est connectée en amont desdits moyens de débrouillage et comporte un registre à décalage (18) dans lequel transitent lesdites informations numériques embrouillées, en ce que lesdits moyens de

débrouillage comportent une sortie où est délivrée ladite clé d'embrouillage (Ce) déchiffrée et en ce qu'un chiffreur interne (Chi) pilote des moyens de forçage dudit registre à décalage, ledit chiffreur interne étant relié à ladite sortie délivrant ladite clé d'embrouillage déchiffrée.

6- Installation selon la revendication 5, caractérisée en ce que le chiffreur interne (Chi) est paramétré par ladite clé d'exploitation interne (Cexi) et délivre des informations de forçage au registre à décalage, représentatif de ladite clé d'embrouillage chiffrée par ladite clé d'exploitation interne, lorsque ledit registre contient des informations de clé d'embrouillage d'une composante d'exploitation (ECM).

FIG.1

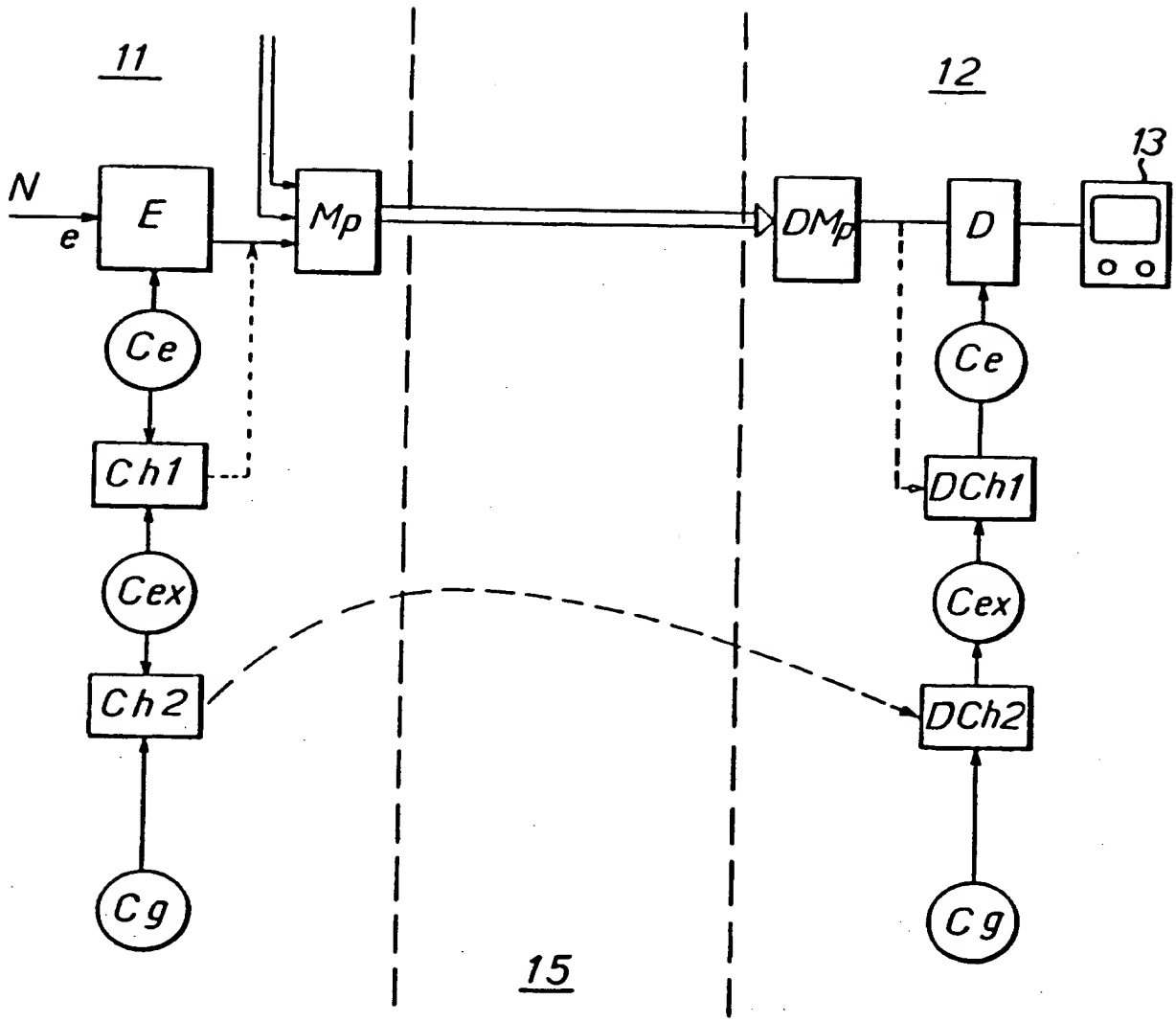


FIG. 2

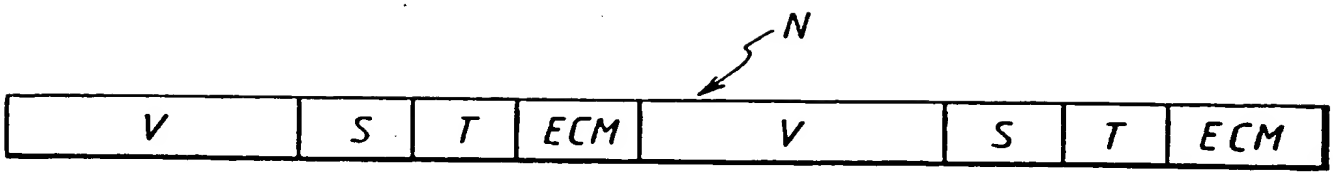
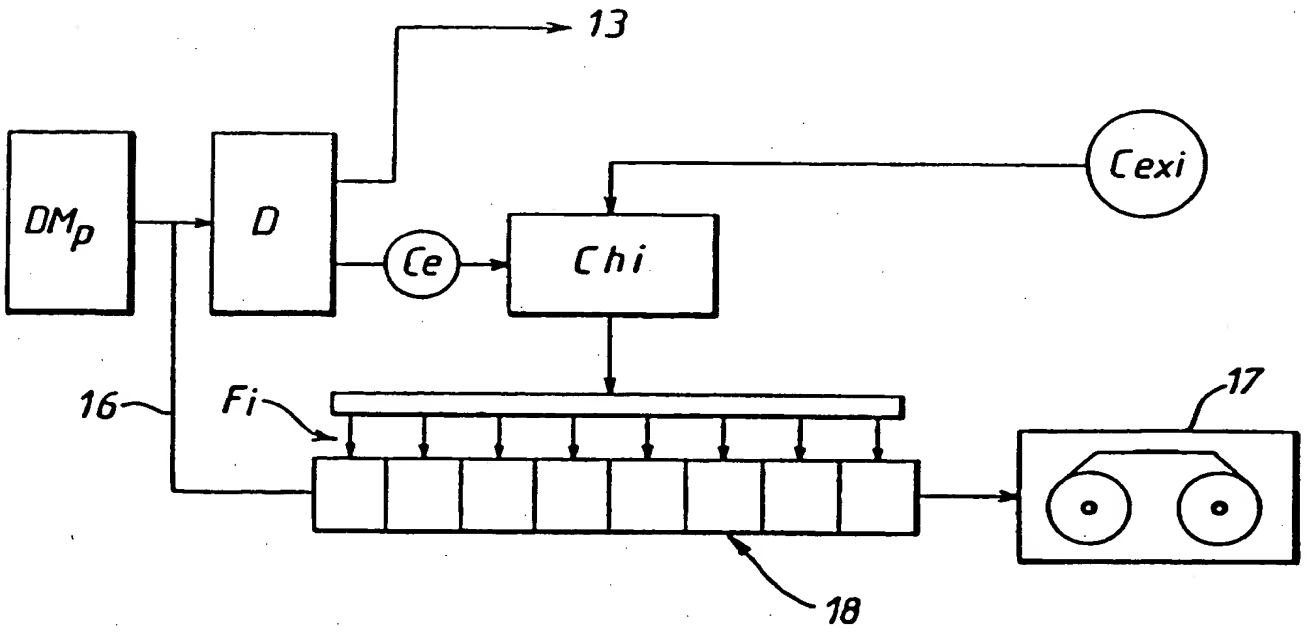



FIG. 3



REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

# RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

2732537

FA 516352
FR 9503859

## DOCUMENTS CONSIDERES COMME PERTINENTS

| Catégorie | Citation du document avec indication, en cas de besoin, des parties pertinentes | Revendications concernées de la demande examinée |
|---|---|---|
| A | CABLE TV SESSIONS, MONTREUX, JUNE 10 - 15, 1993, no. SYMP. 18, 11 Juin 1993 POSTES;TELEPHONES ET TELEGRAPHES SUISSES, pages 761-769, XP 000379391 VIGARIE J P 'A DEVICE FOR REAL-TIME MODIFICATION OF ACCESS CONDITIONS IN A D2-MAC/PACKET EUROCRYPT SIGNAL: THE TRANSCONTROLLER' * le document en entier * --- | 1-6 |
| A | PATENT ABSTRACTS OF JAPAN vol. 014 no. 200 (E-0920) ,24 Avril 1990 & JP-A-02 041051 (MATSUSHITA ELECTRIC IND CO LTD;OTHERS: 01) 9 Février 1990, * abrégé * --- | 1-6 |
| A | US-A-5 230 019 (YANAGIMICHI TOYOKAZU ET AL) 20 Juillet 1993 * abrégé * --- | 1-6 |
| A | EP-A-0 461 029 (MATRA COMMUNICATION ;FRANCE TELECOM (FR); TELEDIFFUSION FSE (FR)) 11 Décembre 1991 * le document en entier * ----- | 1-6 |

DOMAINES TECHNIQUES RECHERCHES (Int.Cl.6)

H04N

1

| Date d'achèvement de la recherche | Examinateur |
|---|---|
| 9 Octobre 1995 | Greve, M |

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)